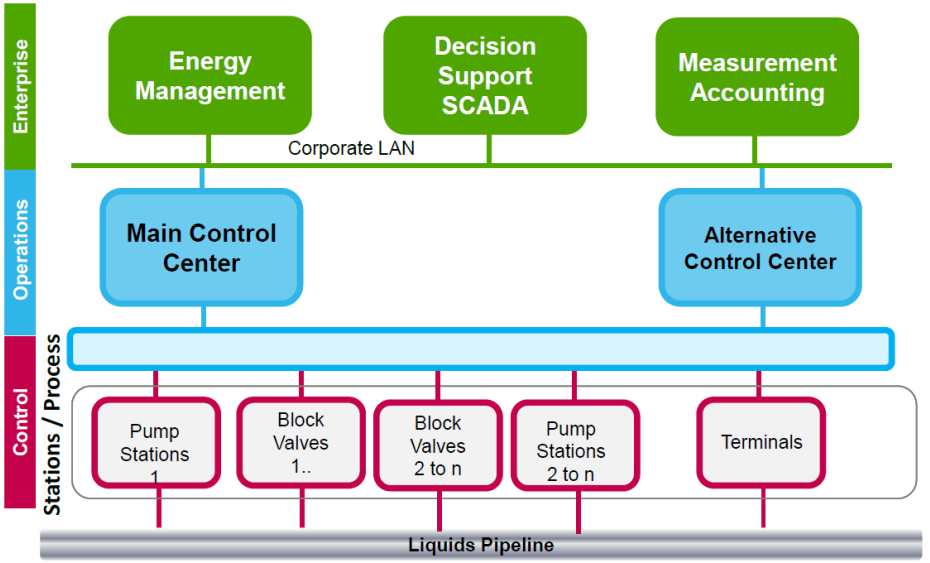
Functional safety and cyber security analysis for life cycle management of industrial control systems in hazardous plants and oil port critical infrastructure including insurance

PRESENTATION AT HAZARD WORKSHOP ORGANIZED BY PSRA ON 15.02.2019 IN GDYNIA

Project Partner:
Polish Safety and Reliability Association (PL)

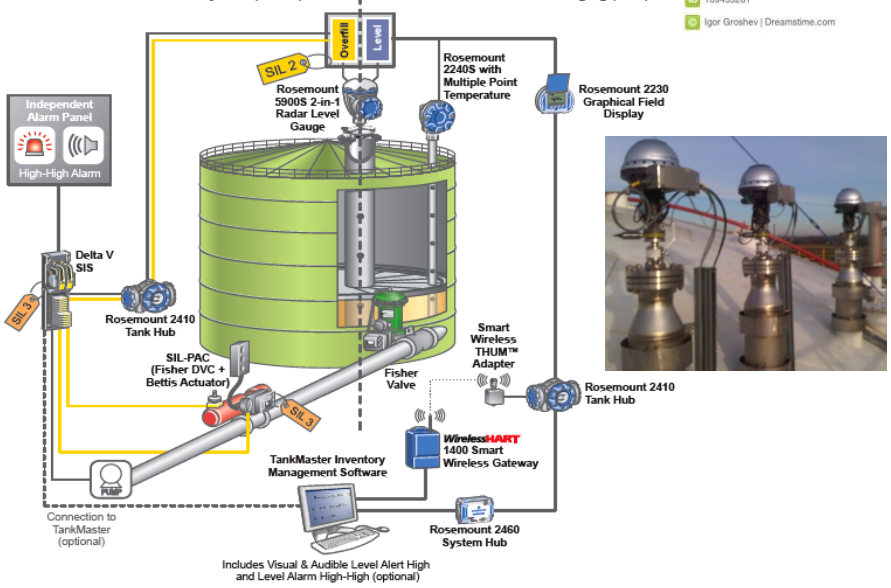
Kosmowski Kazimierz T. (GUT)
Gołębiewski Dariusz (PZU)

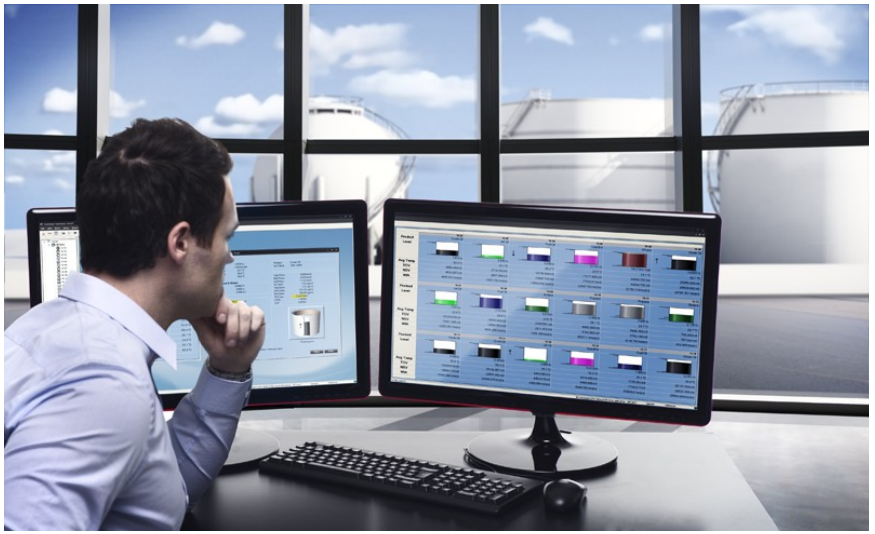
Oil port installations and the DCS / SCADA system and the control system with implemented safety functions



Automatic Overfill Prevention System (AOPS)

Automatic Tank Gauging (ATG)



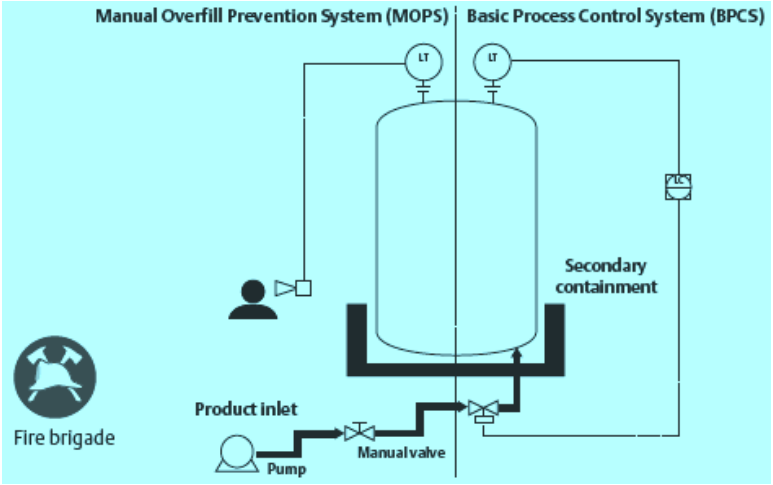


Scope of presentation

- Functional safety requirements after Buncefield accident
- Legal requirements concerning security of networks and information systems
- OT / IT convergence
- Vulnerability of ICS components
- Risk analysis and management in organisations (ISO 31000)
- Individual and societal risk criteria
- Safety and security evaluation - towards integrated approach
- Functional safety and cyber security analysis
- Systemic MTE approach in safety and security analysis and management
- Towards process based management system
- A and B categories of Controls / Barriers (C/B) for defining KPIs
- Examples of performance indicators to be assessed in insurance audit
- Conclusions

IACS (DCS/SCADA-BPCS/SIS) and basic functional safety requirements for Buncefield type sites

1. The Competent Authority and Operators should develop a common methodology to determine SIL requirements for **overfill prevention systems** of tanks in line with the principles of EN 61508 / 61511.
2. **Protection against loss of containment** is required that is physically and electrically separated and independent from the tank gauging system.
3. The safety-related systems should be designed, operated and maintained **to achieve and maintain required SIL** *(safety integrity level)* in accordance with the requirements of the standard EN 61511.
4. **All elements of an overfill prevention system should be proof tested** in accordance with the validated arrangements and procedures sufficiently frequently to ensure that specified SIL is maintained in practice in accordance with the requirements of Part 1 of EN 61511
5. The sector should put in place arrangements **to ensure the receiving site has ultimate control of tank filling**. The receiving site should be able to **safely terminate or divert a transfer** (to prevent loss of containment or other dangerous conditions) **without depending on the actions of a remote third party, or on the availability of communications to a remote location.**



Legal requirements concerning security of networks and information systems in EU including cyber security of ports

NIS Directive

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a **high common level of security of network and information systems** across the Union

Maritime (ISPS Code) Regulations 2014, Legal notice No. 102, **Maritime Transport Decree** No. 20 of 2013.

Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on **enhancing ship and port facility security** (OJ L 129, 29.4.2004, p. 6).

Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on **enhancing port security** (OJ L 310, 25.11.2005, p. 28).

NIS
Network and Information Security

CERT
Computer Emergency Response Team

CSIRT
Computer Security Incident Response Team

csirt.gov.pl (Poland)

ISPS Code basic requirements

The persons carrying out the assessment shall have appropriate skills to evaluate **security of the port facility**, taking into account following elements:

(a) physical security;

(b) **security equipment**;

(c) **security procedures**;

(d) **radio communications systems** (including **IT systems and networks**);

(e) transportation infrastructure;

(f) utilities infrastructure;

(g) other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations within the port, port facility or aboard ships adjacent thereto; and

(h) available expert assistance.

SOC
Security Operations Center

SIEM
Security Information and Event Management

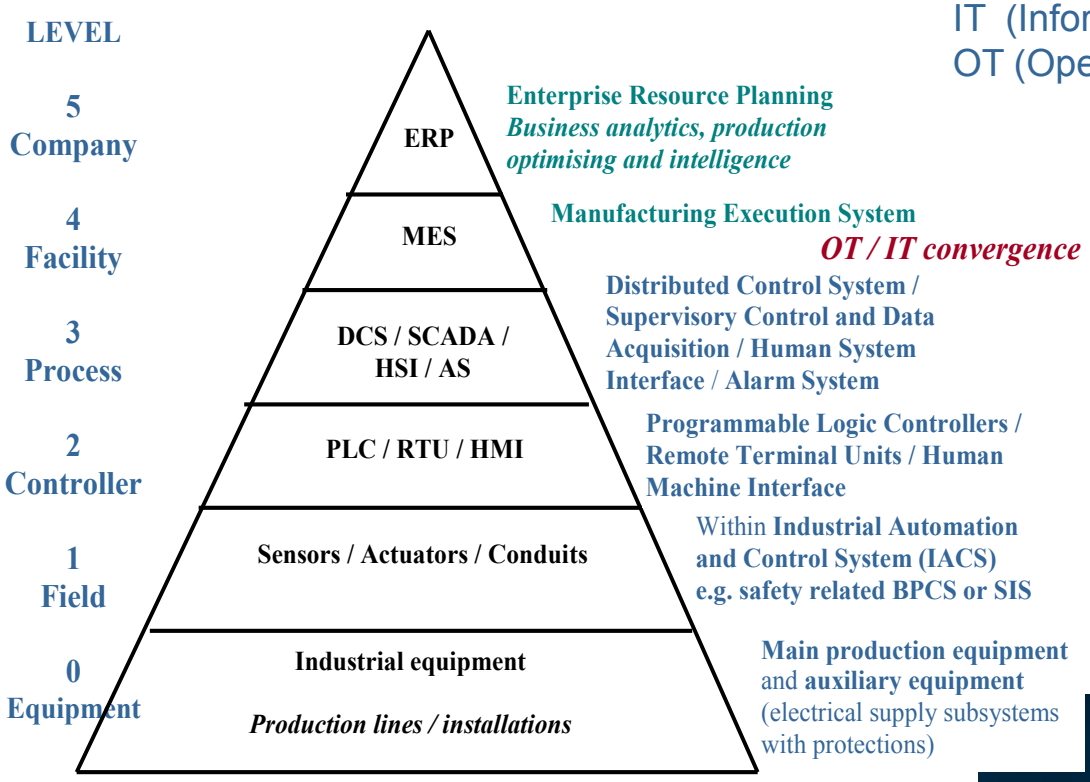
Assets and infrastructure that should be considered as important to protect (Regulation EC No 725/2004)

- Accesses, entrances, approaches, and anchorages, manoeuvring and berthing areas;
- Cargo facilities, terminals, storage areas, and cargo handling equipment;
- **Systems such as electrical distribution systems, radio and telecommunication systems and computer systems and networks;**
- Port vessel traffic management systems and aids to navigation;
- Power plants, cargo transfer piping, and water supplies;
- Bridges, railways, roads;
- Port service vessels, including pilot boats, tugs, lighters, etc.;
- **Security and surveillance equipment and systems**; and
- The waters adjacent to the port facility.

The port facility security assessments shall be **reviewed and updated annually** taking into account:

- **changing threats and/or minor changes** in the port facility, and
- shall **always be reviewed and updated when major changes** to the port facility take place.

Typical levels in an industrial process plant and its control system (IACS) in the context of IT / OT convergence



Enterprise Resource Planning
Business analytics, production optimising and intelligence

Manufacturing Execution System

OT / IT convergence

Distributed Control System / Supervisory Control and Data Acquisition / Human System Interface / Alarm System

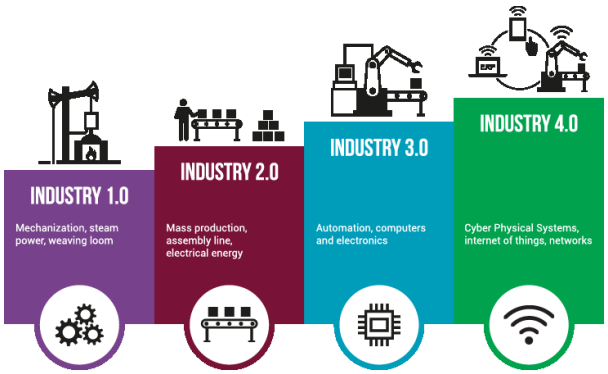
Programmable Logic Controllers / Remote Terminal Units / Human Machine Interface

Within **Industrial Automation and Control System (IACS) e.g. safety related BPCS or SIS**

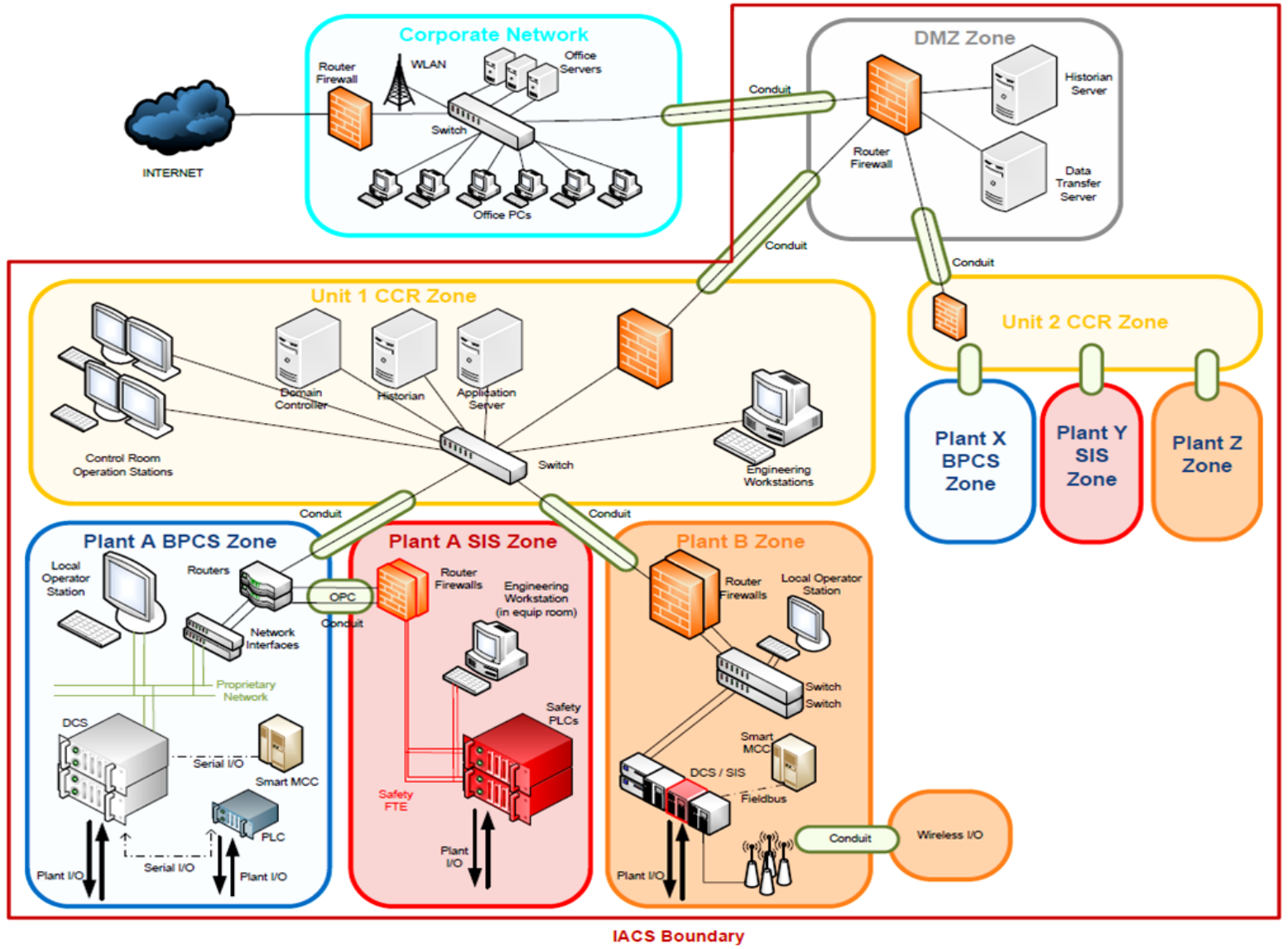
Main production equipment and **auxiliary equipment** (electrical supply subsystems with protections)

IT (Information Technology) / OT (Operational Technology)

Technology evolution - **Industry 4.0 concept**

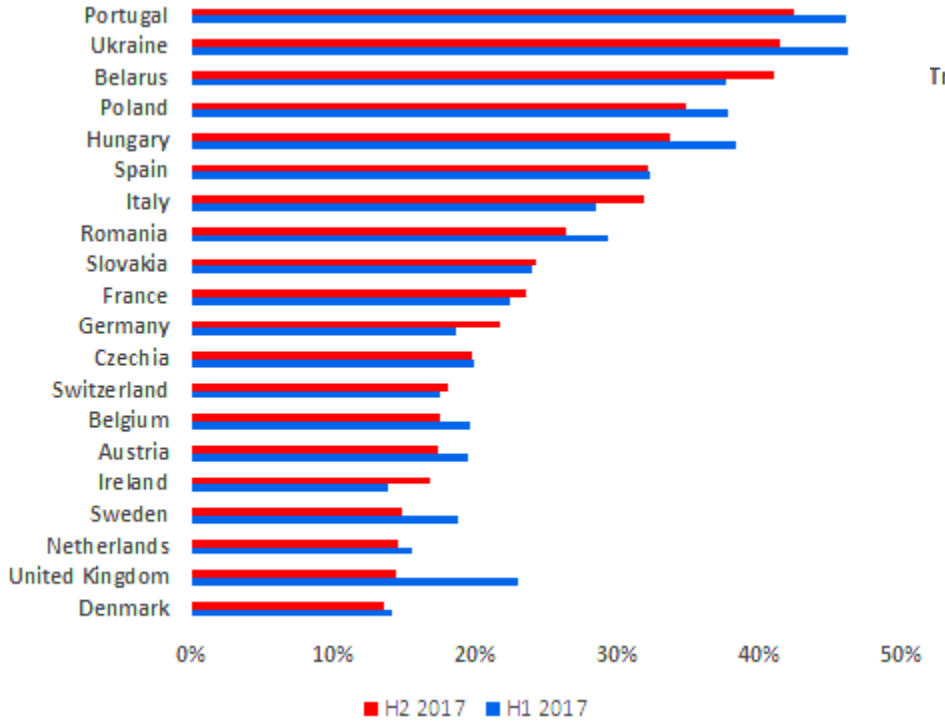


Typical Industrial Control System (ICS) for a large site and Demilitarized Zone (DMZ)

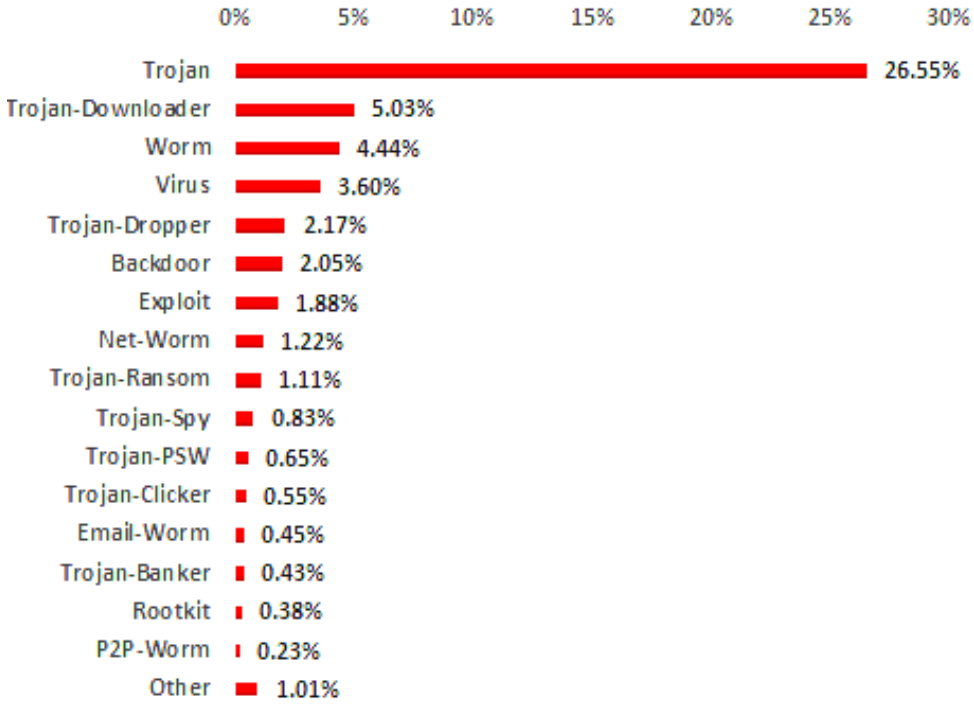


Source: Cyber Security for Industrial Automation and Control Systems (IACS). HSE report for Chemical Explosives and Microbiological Hazards Division (CEMHD) and Energy Division, Electrical Control and Instrumentation (EC&I) Specialist Inspectors.

Problems of ICS computers being attacked in Europe

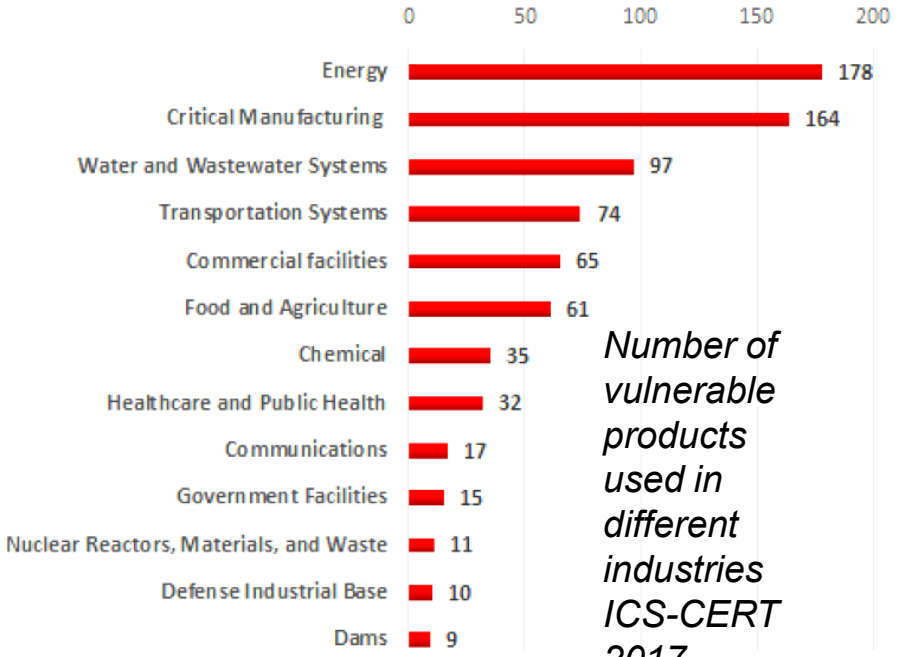


Percentage of attacked ICS computers in Europe H2 2017 vs H1 2017 (Kaspersky Lab)

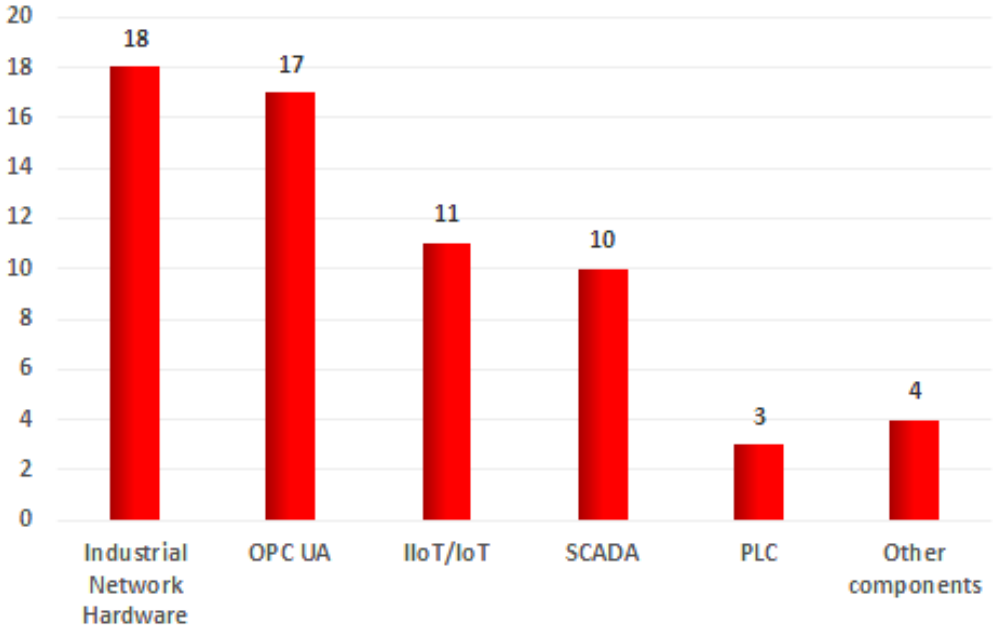


Malware classes, percentage of ICS computers attacked, H2 2017 (Kaspersky Lab)

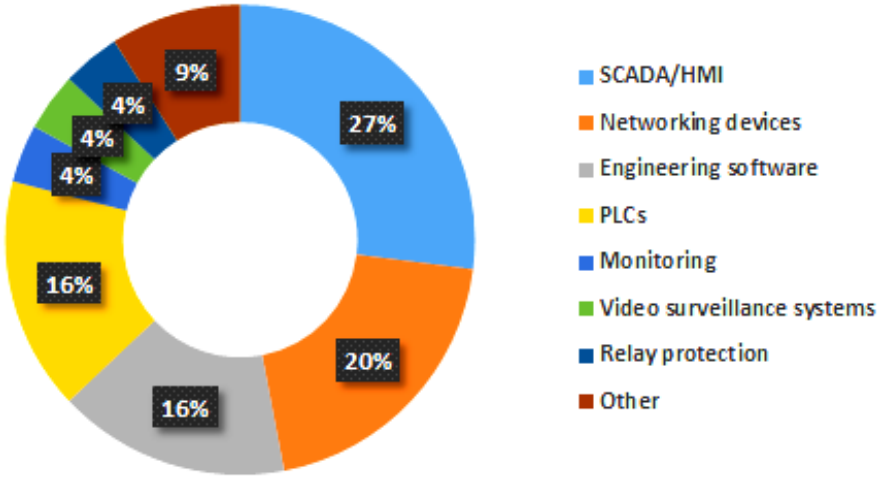
Vulnerability of ICS components



Number of vulnerable products used in different industries ICS-CERT 2017

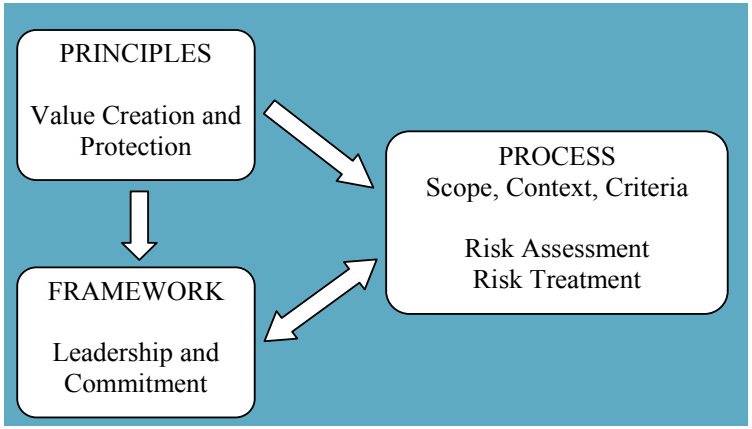


Distribution of vulnerabilities identified by Kaspersky Lab ICS CERT in 2017 by types of components analyzed



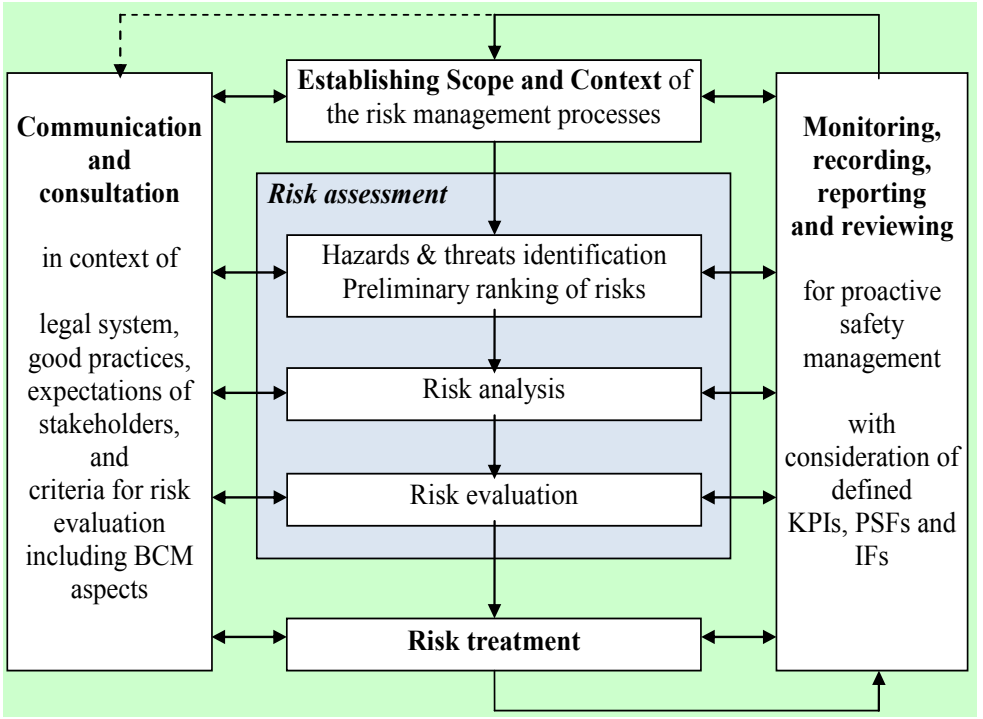
Distribution of vulnerabilities identified by ICS components

Risk analysis and management in organisations (ISO 31000)

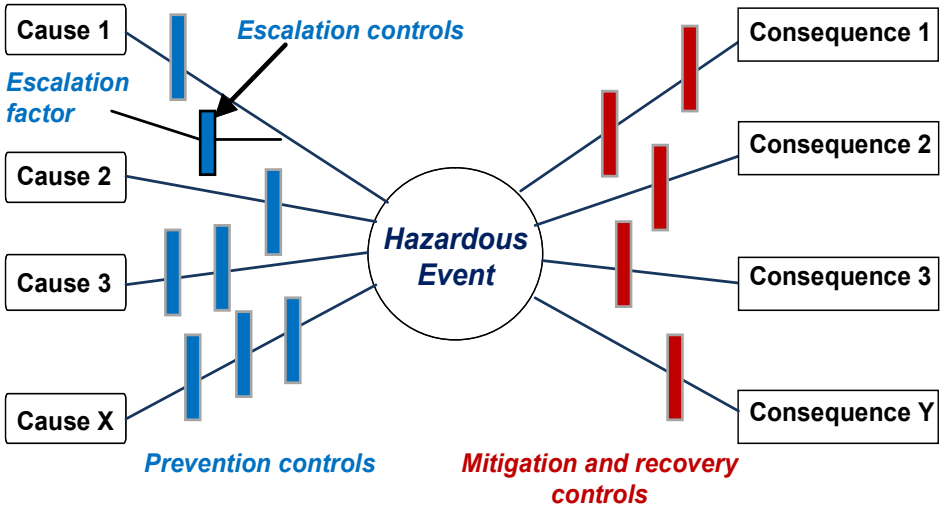


Relations between principles, framework and process in the risk management

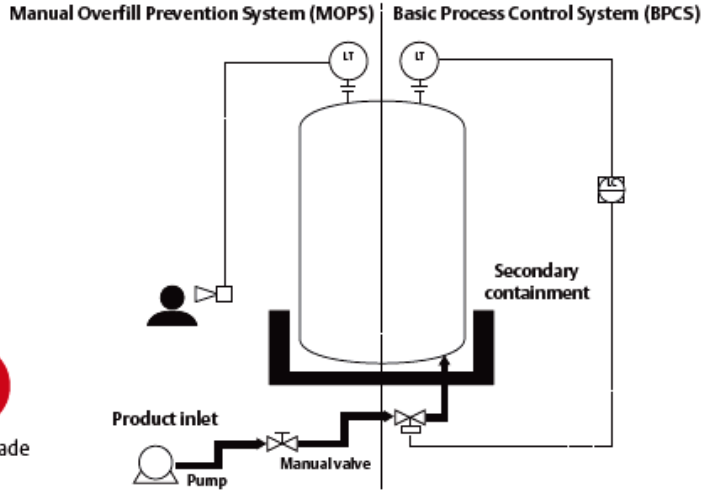
Risk management process in life cycle

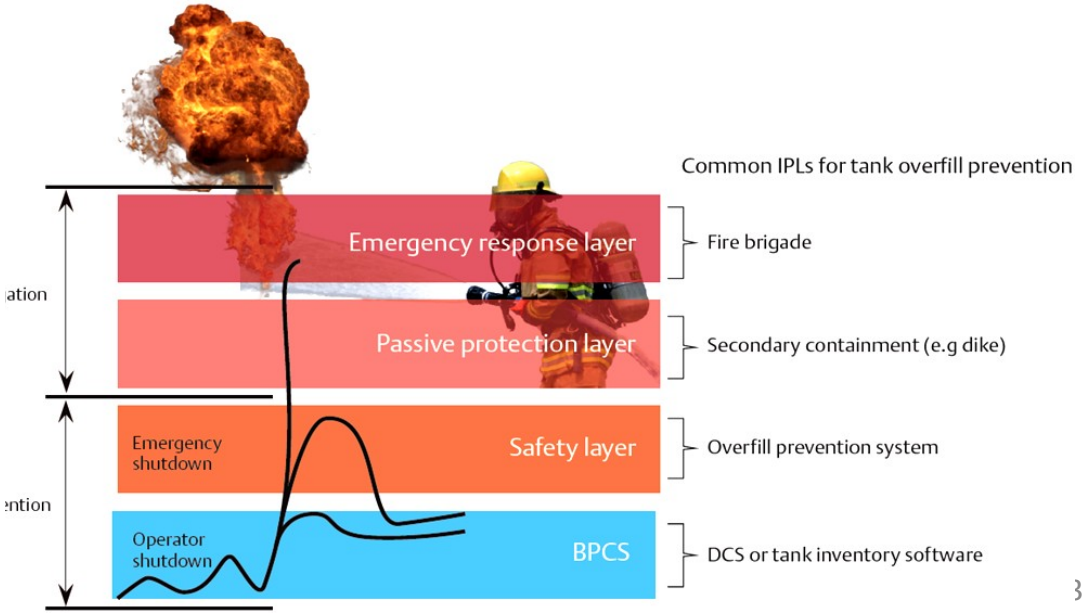


Prevention and mitigation controls for reducing risks: probabilities / frequencies and consequences of scenarios (categories for representation of potential accidents)



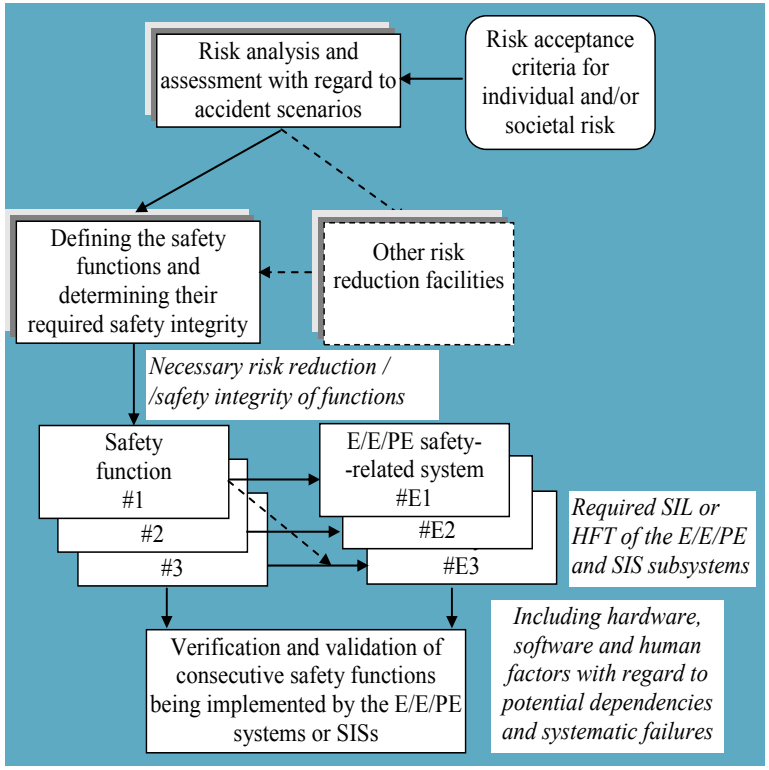
Based on ISO 31010





Fire brigade

Functional safety and cybersecurity analysis within process based management system



Allocation of requirements
for safety-related systems: E/E/PE or SIS
according to EN 61508/61511

Functional safety standards EN 61508, 61511; technical specification and risk-related criteria; methods for modeling and evaluating consequences and frequencies of accident scenarios in the context of protection layers and rings

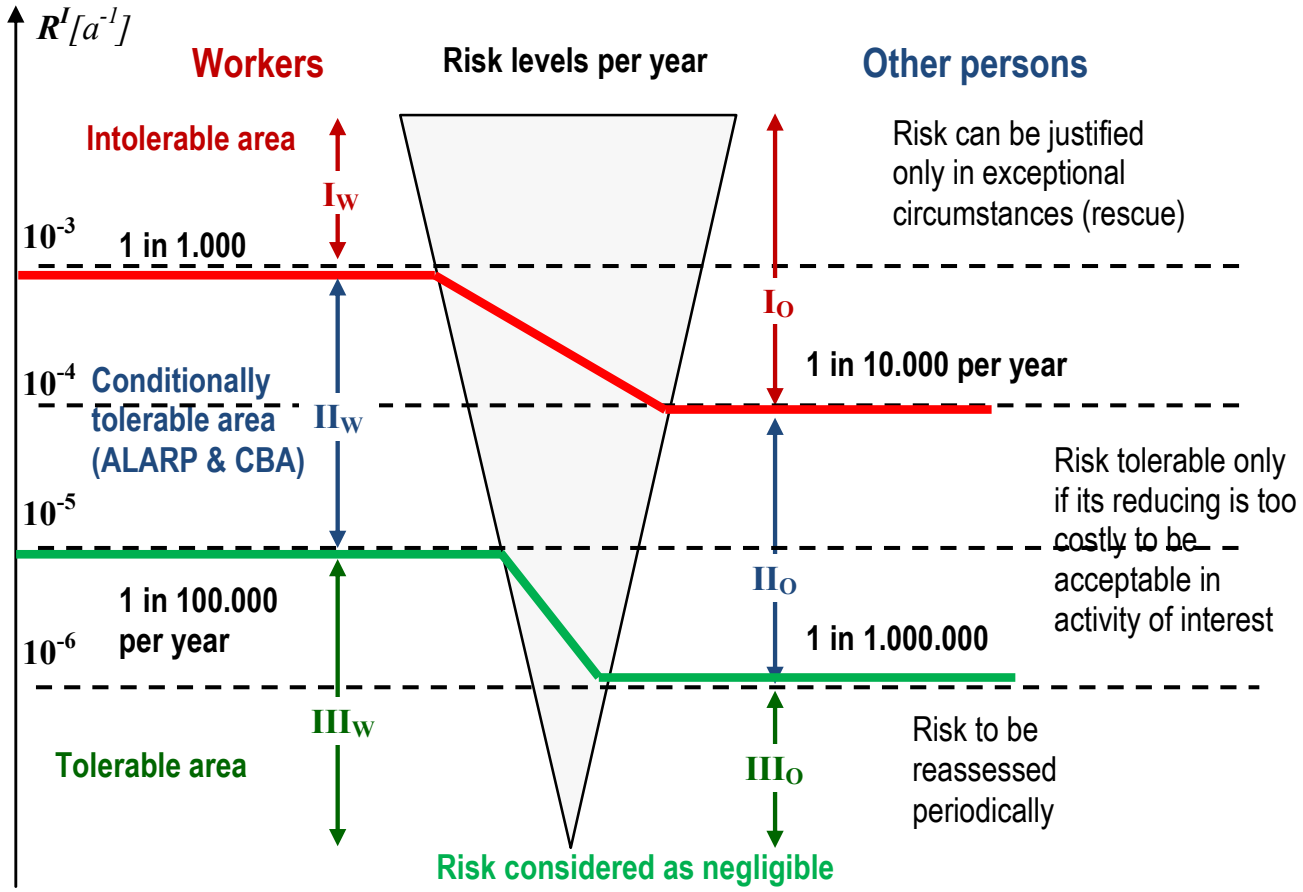
Process based management system (PBMS) including functional safety and security aspects; evaluation of a set of key performance indicators (KPIs) in given hazardous process plant / fuel base / oil terminal

Analysis of hazards / threats and evaluation of risks for determining and verifying SIL of safety functions implemented using BPCS, AS and SIS and working out testing and maintenance strategy; decision making under uncertainty in life cycle; *updating relevant data and knowledge bases for plant specific evaluation*

1. Knowledge & methods for hazards analysis and risk evaluation, process safety management (PSM), business continuity management (BCM)	ISO 31000, 31010 ISO 22031 OSHA 3132 ISO 28000 OHSAS 18001 ISO 45001
2. Knowledge & methods suitable for the development and usage the quality, environment and safety / security management systems	EN ISO 9001 EN ISO 14001 EN/IEC 27001 ISO/IEC 26702
3. Knowledge & methods for identification of hazards, analyses and assessments of risks; designing the protection layers and rings	PHA HAZOP, HAZID FMECA, FTA, ETA LOPA, SeSa
4. Knowledge & methods for security analysis of computer systems / networks and software quality/safety management	ISO/IEC 27001 ISO/IEC 27005 ISO/IEC 15408 (CC) IEC 62443 IEC 62280
5. Knowledge & methods suitable for designing interactive HMI/HSI, the control room and alarm system with relevant diagnostics tools	EN ISO 9241-210 EEMUA, ISO 11064 ANSI/ISA 18.02 NUREG-0700
6. Knowledge & methods for assessment of human factors, cognitive task analysis (CTA) and human reliability analysis (HRA)	HTA, TLA, CES HCR, CREAM, HEART THERP, SPAR-H
7. Knowledge & methods supporting cost-benefit analysis (CBA) of risk reduction measures, and scheduling preventive maintenance and overhauls	ALARP R^2P^2, TOR RCM, RBI RIMAP

Sources of knowledge
and selected standards

Threshold levels of individual risk considered in ALARP *(as low as reasonably practicable)* analysis



Based on: ADNOC Group Health, Safety and Environmental Management Guidelines. HSE Risk Management, 2000

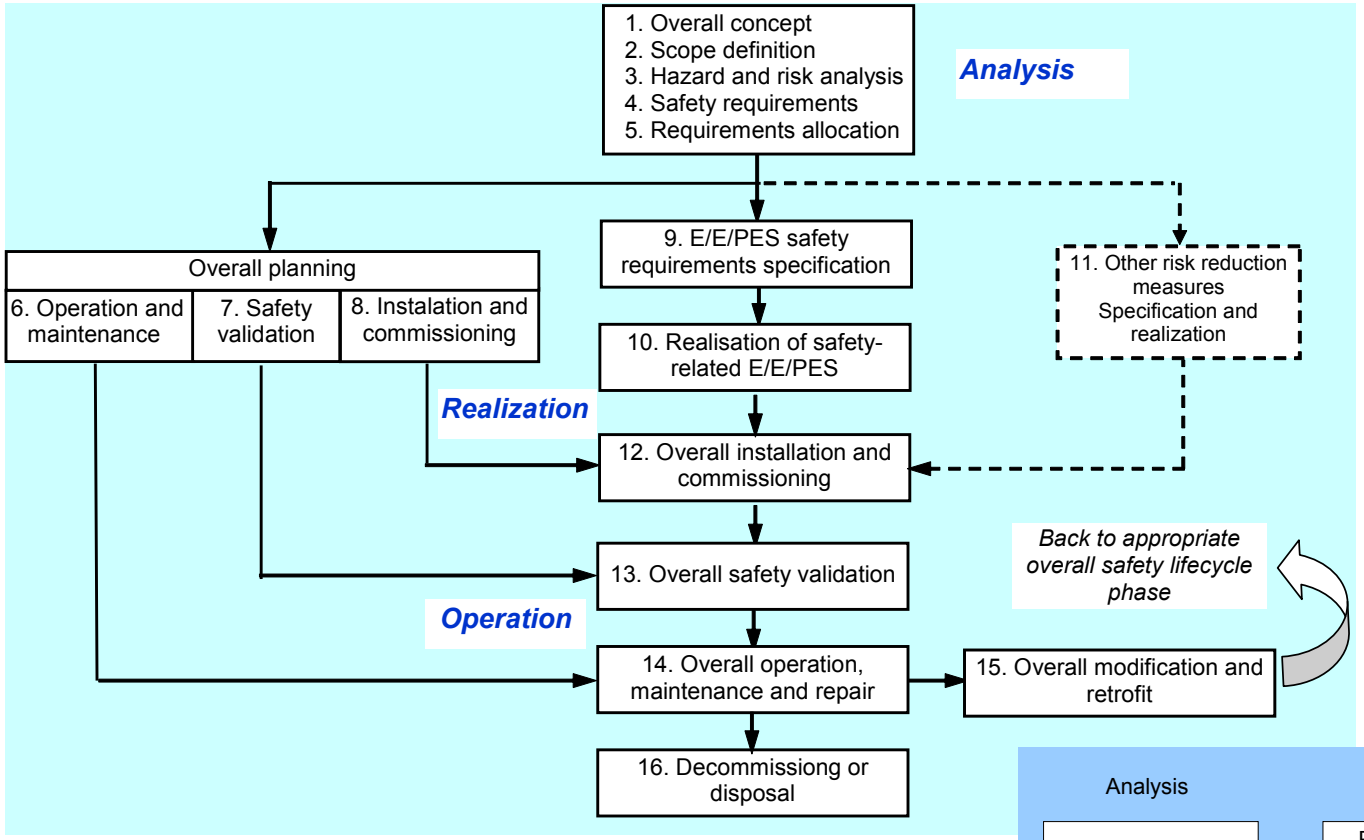
Risk matrix for societal risk assessment and management in the context of functional safety (SIL)

Consequences*					Probability / frequency [a^{-1}]				
					A	B	C	D	E
People – health	**Assets**	**Environment**	**Reputation**	**Severity**	$F_A < 10^{-4}$ **Improbable**	$F_B < 10^{-3}$ **Remote**	$F_C < 10^{-2}$ **Occasional**	$F_D < 10^{-1}$ **Probable**	$F_E \geq 10^{-1}$ **Frequent**
Multiple fatalities **(< 10^{-5} a^{-1})**	Extensive damage **(≥ $100M)**	Massive effect	Catastrophic (international impact)	**5**	**RR*$_{5A}$**	**RR*$_{5B}$**	**RR*$_{5C}$**	**RR*$_{5D}$**	**RR*$_{5E}$**
Single fatality **(< 10^{-4} a^{-1})**	Major damage **(< $100M)**	Major effect	Severe (national impact)	**4**	**RR*$_{4A}$**	**RR*$_{4B}$**	**RR*$_{4C}$**	**RR*$_{4D}$**	**RR*$_{4E}$**
Major injury **(< 10^{-3} a^{-1})**	Local damage **(< $10M)**	Localised effect	Considerable impact	**3**	**RR*$_{3A}$**	**RR*$_{3B}$**	**RR*$_{3C}$**	**RR*$_{3D}$**	**RR*$_{3E}$**
Minor injury **(< 10^{-2} a^{-1})**	Minor damage **(< $1M)**	Minor effect	Minor impact	**2**			**RR*$_{2C}$**	**RR*$_{2D}$**	**RR*$_{2E}$**
Slight injury **(< 10^{-1} a^{-1})**	Slight damage **(< $100k)**	Slight effect	Slight impact	**1**				**RR*$_{1D}$**	**RR*$_{1E}$**
No injuries	No damage	No effect	No impact	**0**					

Required risk reduction	Probability of Failure on Demand – average for coasidered safety function	Safety Integrity Level
RR = 10	**$PFD_{avg} = 10^{-1}$**	**SIL1**
RR = 100	**$PFD_{avg} = 10^{-2}$**	**SIL2**
RR = 1000	**$PFD_{avg} = 10^{-3}$**	**SIL3**
RR = 10000	**$PFD_{avg} = 10^{-4}$**	**SIL4**

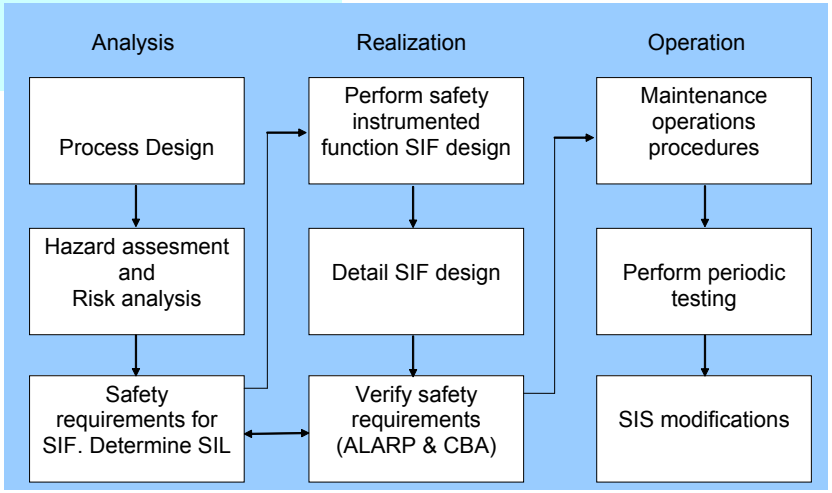
	Intolerable too high risk
	Conditionally tolerable risk - reduction required (ALARP & CBA)
	Tolerable risk (periodically reassessed)

Functional safety management in lifecycle



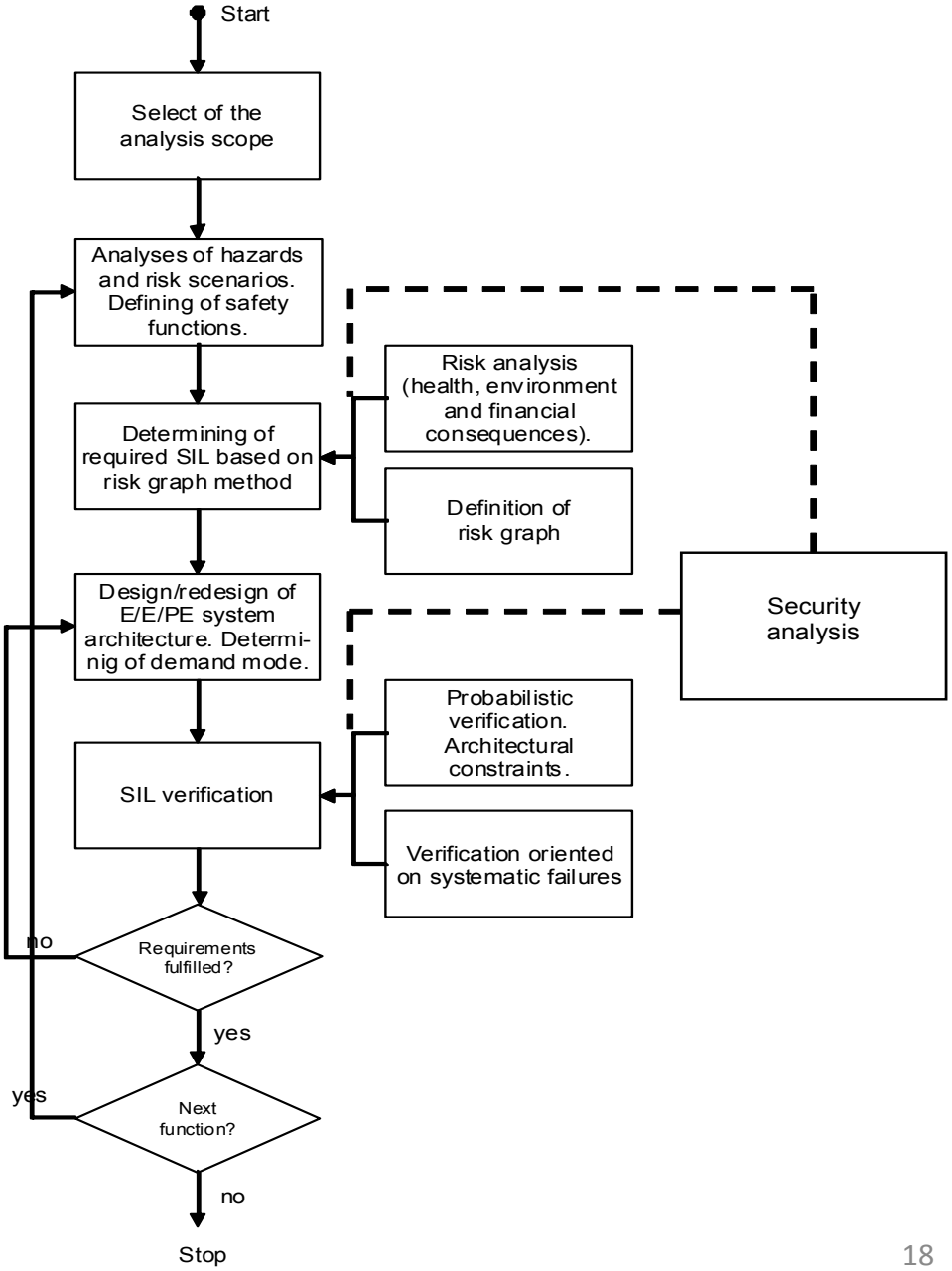
Based on IEC 61508 (2010)

The design, operation, periodical testing and maintenance of E/E/PES: Electric / Electronic / Programmable Electronic (E/E/PE) Systems

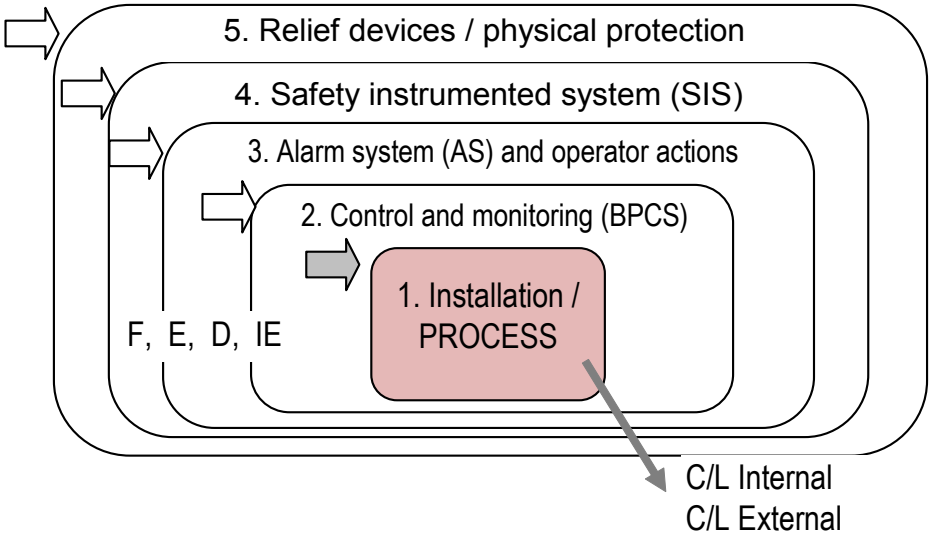


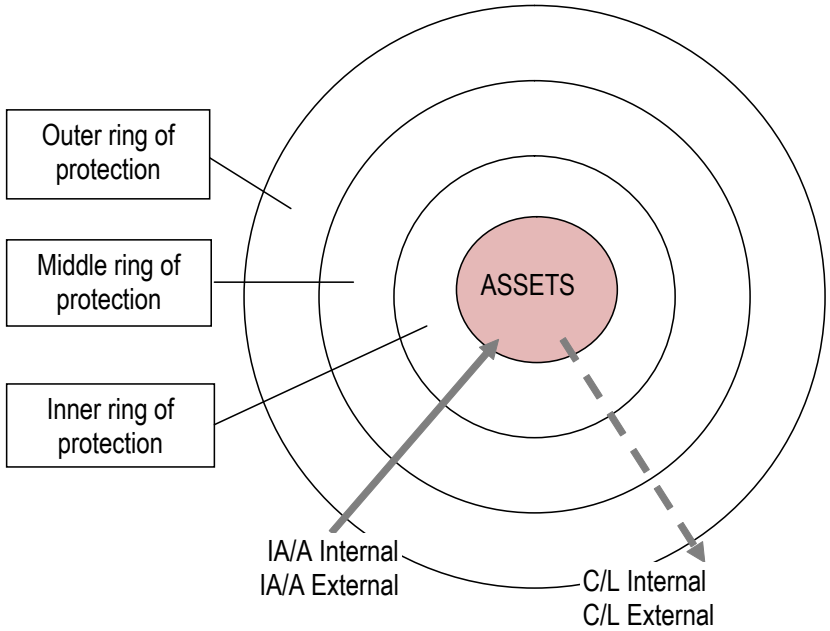
Integrated functional safety and cyber security analysis procedure

1. Define the safety functions for reducing relevant risks taking into consideration the results of identification and evaluation of hazards.
2. Determine required safety integrity level SIL (1÷4) of consecutive safety functions based on the results of risk assessment using quantitative risk analysis method or semi-quantitative method, e.g. calibrated risk graph for defined consequences.
3. Design appropriate architecture of E/E/PE safety-related systems or SISs for implementing relevant safety functions.
4. Verify SIL / SAL of safety-related systems using quantitative probabilistic modeling methods for architectures of E/E/PE or SIS designed with regard to architectural constrains - the interval probabilistic criteria for SILs are defined in EN 61508 and EN 61511 standard.
5. Consider security related aspects for the control safety-related systems operating in computer networks with regard to IEC 62443.



Hazards / threats and typical protection layers / rings in industrial hazardous installations / plants





Protection layers

F-failures, E-errors, D-disturbances, IE-initiating events
C-consequences, L-losses

Protection rings

IA-intentional act, A-attack, I-incident

The *outer ring* may include: *lighting, fences, entrance/exit points, bollards, intrusion detection sensors and smart alarming, guards on patrol at property fence line*, etc.
The *middle ring* may include: *escort of visitors, locked doors, receptionist, access control system, window bars, parcel inspection, turnstiles*, etc.
The *inner ring* may include technical and organizational solutions as*: door and cabinet locks, visitor escort policies, emergency communications, secure computer rooms, network firewalls and passwords policy*, etc.

Examples of Key Performance Indicators (KPIs) for BPCS, AS and SIS

Basic Process Control System (BPCS)

***BPCS-1**: Mean time to dangerous failure ($MTTF_D$),*
***BPCS-2**: Mean time to abnormal performance requiring correction ($MTTF_C$),*
***BPCS-3**: Safe failure fraction (S_{FF}) for architectures performing safety function,*
***BPCS-4**: Mean time to spurious operation failure ($MTTF_S$),*
***BPCS-5**: Period of the control room audit and review of functional safety procedures.*

Alarm system (AS)

***AS-1**: Alarm rates in normal operation per day (maximum and average),*
***AS-2**: Number of alarms following an upset situation per hour,*
***AS-3**: Percentage of hours containing more than 30 alarms,*
***AS-4**: Percentage of 10-minute periods containing more than 5 alarms,*
***AS-5**:Percentage of time the alarm system is in a flood condition,*

Safety Instrumented System (SIS)

***SIS-1:** The number of demands on the SIS with implemented safety function,*
***SIS-2:** The time intervals of partial and overall testing of the redundant SIS,*
***SIS-3:** The number of failures of channels on tests in redundant SIS per month,*
***SIS-4:** Spurious operation rate of SIS channels per months,*
***SIS-5**: Safe failure fraction (S_{FF}) for subsystems of the safety-related system.*

IACS cyber security related performance indicators (IEC 62443)

***Security level* (SL)** concept provides a qualitative approach to addressing security for a **ICS zone:**

SL 1 for protection against casual or coincidental violation,

SL 2 for protection against intentional violation using simple means with low resources, generic skills and low motivation,

SL 3 for protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation,

SL 4 for protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation.

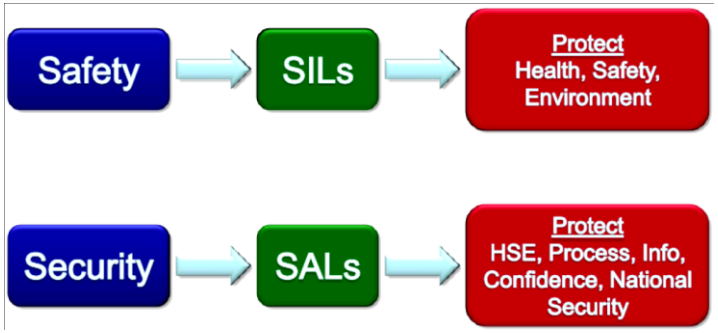
Three **categories** of SLs are distinguished:

SL-C (Capability) - A particular component or system is capable of being configured by an asset owner or system integrator to protect against a given type of threat,

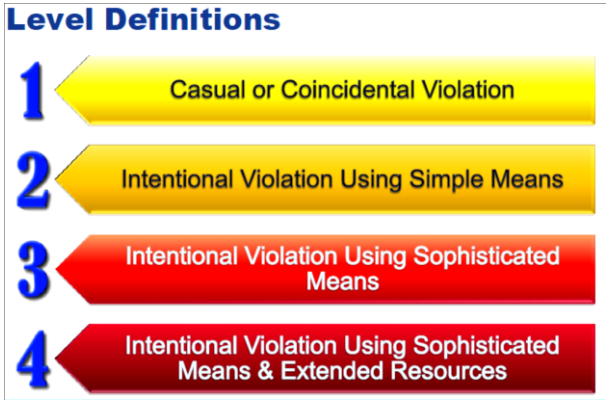
SL-T (Target) - The asset owner or system integrator has determined through a risk assessment that they need to protect this particular zone, system or component against this level of threat,

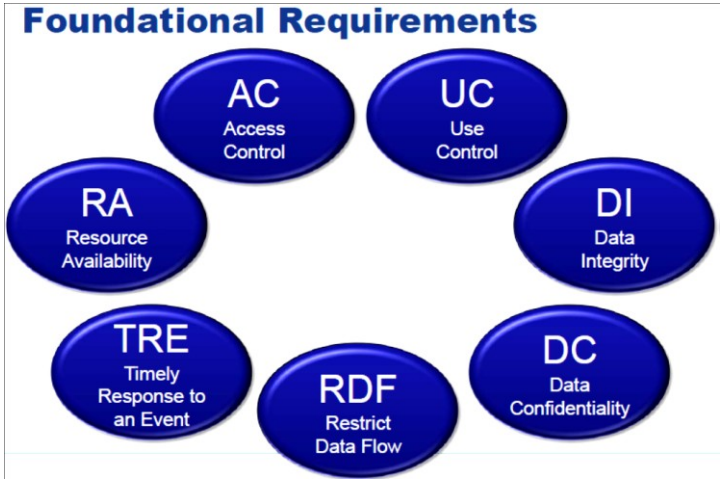
SL-A (Achieved) - The asset owner, system integrator, product supplier and/or any combination of these has configured the zone, system or component to meet the particular security requirements defined for that SL.

Security Assurance Levels (SALs) in the context of Fundamental Requirements (FRs): target and achieved



Safety Integrity Level SIL
Security Assurance Level SAL





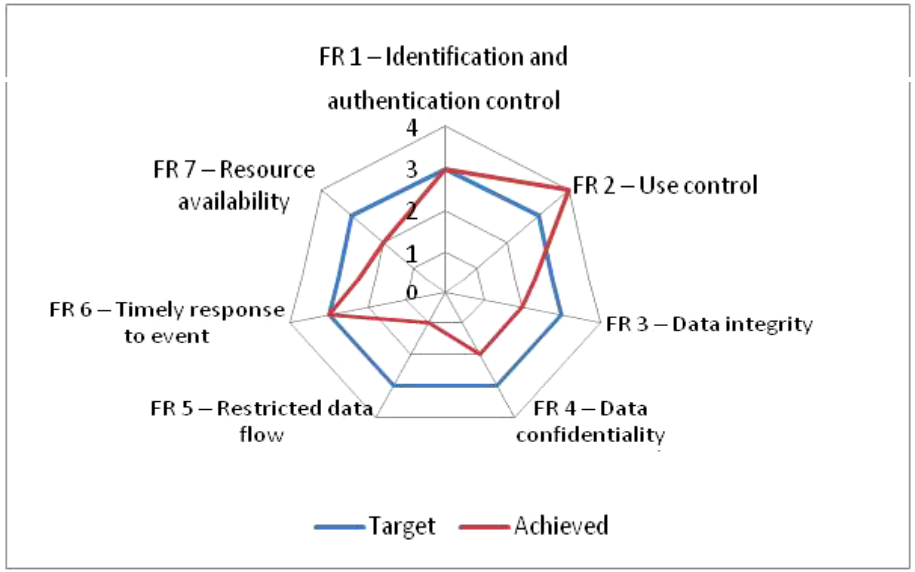
SAL Vector Format

$$SAL\text{-}?([FR,]domain) = \{AC \;\; UC \;\; DI \;\; DC \;\; RDF \;\; TRE \;\; RA\}$$

- Examples
  - SAL-T(Control System Zone) = {2 2 0 1 3 1 3}
  - SAL-C(Engineering Workstation) = {3 3 2 3 0 0 1}
  - SAL-C(RA, Safety PLC) = 4
- Definition & usage still under development

Source: Gilsinn J., Schierholz R.: Security Assurance Levels: A Vector Approach. NIST, ABB 2010.

Security Assurance Levels (SALs) in the context of Fundamental Requirements (FRs): Target and Achieved (cont.)



If *Achieved* SAL < *Target* SAL
some additional **countermeasures**
have to be considered
in the implementation process.

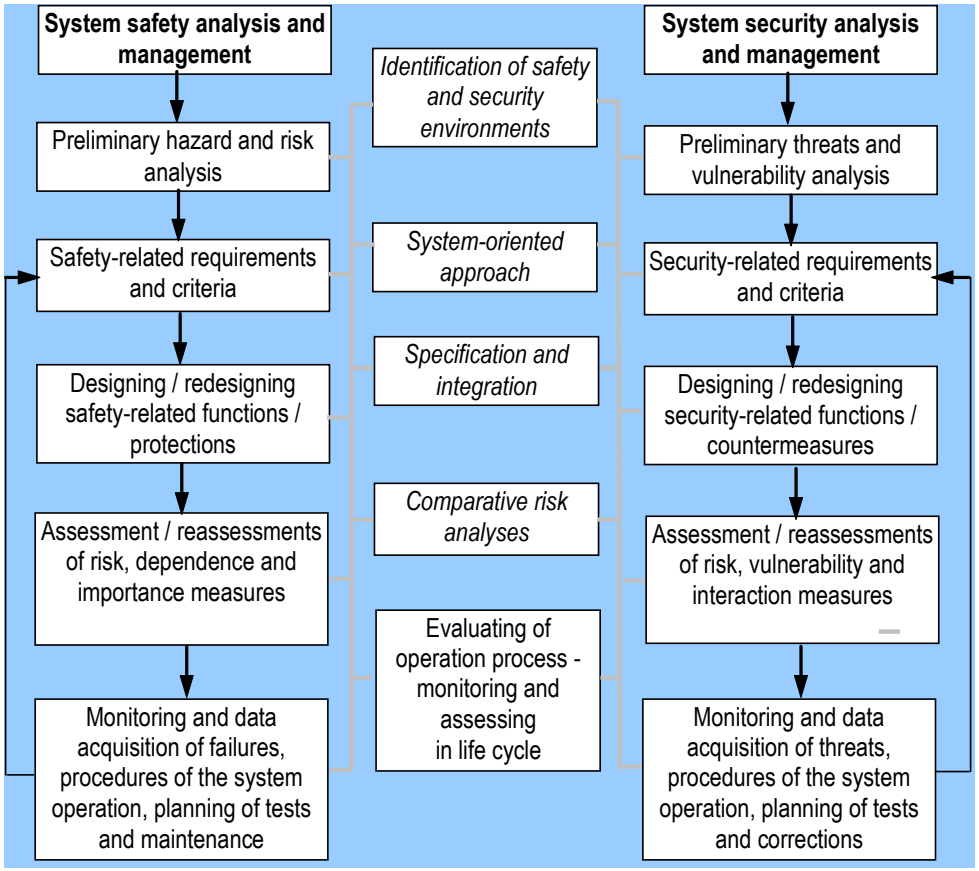
The countermeasures to be implemented for increasing SAL include:

- **technical measures** (antivirus, antispyware, firewalls, encryption, virtual private networks - VPN, passwords, authentication systems, access control, intrusion detection and prevention, network segmentation, etc.),
- **security management** (rights management, patch management for system & application, security incident management, training, etc.).

One of countermeasures to be considered is a ***demilitarized zone*** **(DMZ)** that aims to enforce the control network's policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the control network from outside attacks.

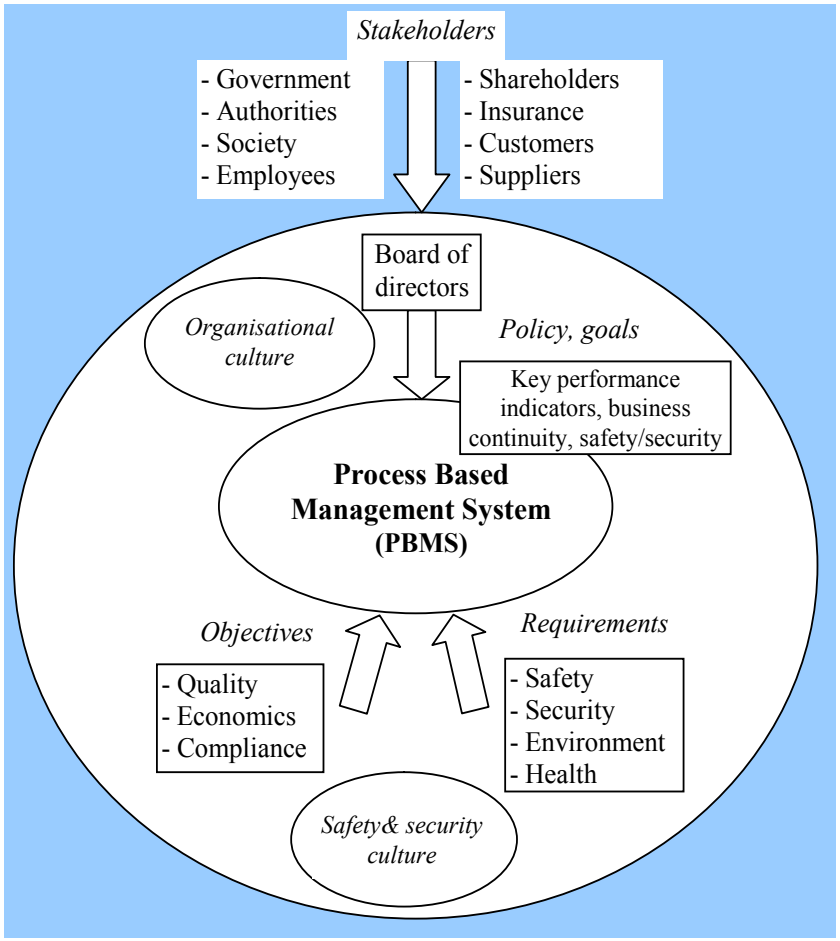
Source: Jean-Pierre Hauet: ISA99/IEC 62443: a solution to cyber-security issues? KB Intelligence Standards Certification Education & Training, ISA District 12 VP, 2012.

Integrated functional safety and cyber security analysis of critical systems

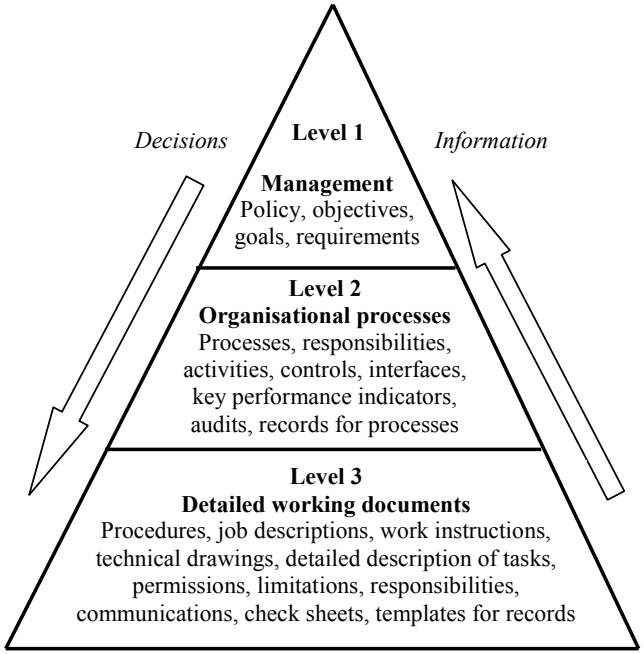


SIL & SAL for **risk levels**		Criticality of consequences			
		Minor	*Low*	*Major*	*Severe*
Probability	*High*	***MR*** SIL 2 SAL 2+	***HR*** SIL 3 SAL 3+	***VHR*** SIL 4 SAL 4	***VHR*** SIL 4 SAL 4
	Medium	***MR*** SIL 2 SAL 2+	***HR*** SIL 3 SAL 3+	***VHR*** SIL 4 SAL 4	***VHR*** SIL 4 SAL 4
	Low	***LR*** SIL 1 SAL 1+	***MR*** SIL 2 SAL 2+	***HR*** SIL 3 SAL 3+	***HR*** SIL 3 SAL 3+
	Rare	***LR*** SIL 1 SAL 1+	***LR*** SIL 1 SAL 1+	***MR*** SIL 2 SAL 2+	***HR*** SIL 3 SAL 3+

Towards process based management system for an oil port infrastructure



Conditions and sources of requirements influencing a process based management system



A hierarchy of decisions, information flow, documents and activities in a process based management system

Examples of processes to be considered for developing the process based management system (PBMS) e.g. for the oil port infrastructure

Executive Processes (EP:)

EP1 Managing the organization and business continuity,
EP2 Managing the processes and procedures,
EP3 Evaluating in time and improving defined KPIs,
EP4 Coordinating external relations including regulators, stakeholders, etc,

Core Processes (CP):

CP1 Monitoring operation of installations, equipment and infrastructure,
CP2 Scheduling services, tests and establishing maintenance programs,
CP3 Monitoring environmental conditions, emissions and effluents,
CP4 Managing operation and assessing safety and vulnerability of installations, and site physical security,
CP5 Managing security of organization's computer system and network,
CP6 Evaluating functional safety and cyber security of IACS, etc,

***Support Processes (SP)**:*

SP1 Providing human resources and training,
SP2 Providing personnel occupational health and safety services,
SP3 Providing IT services and updating software and protection equipment,
SP4 Providing procurement and contracting,
SP5 Providing environmental and emergency services, etc.

Examples of procedures (PR) of interest in practical realization of relevant management processes

PR1 Evaluation of indicators, factors and risks relevant to BCM,
PR2 Evaluation of overfill and leak related risks of terminal tanks,
PR3 Evaluation of individual, social and operational risks for oil port terminal,
PR4 Evaluation of long distance piping operational risks,
PR5 Evaluation of functional safety in life cycle of the control / protection systems for planning tests and preventive maintenance of equipment,
PR6 Evaluation of protection layers including alarm system and HMI,
PR7 Periodic human task analysis in context of communication and interfaces for supporting Human Reliability Analysis (HRA) and planning training to limit human error probability (HEP),
PR8 Periodic integrated functional safety and cyber security evaluation for life cycle IACS management including testing and preventive maintenance of components,
PR9 Staff and personnel recruitment, training and competence management,
PR10 Audit of organizational culture for shaping safety and security culture,
PR11 Evaluation and ranking KPIs and aggregated factors for development strategy and tactic of the risk management (to specify risks for reduction, retention and transfer to the insurance company).

Remark: Procedures are used as specified and have to periodically reviewed as defined in PBMS, e.g. immediately when changes are introduced.

Key performance indicators (KPIs) for proactive safety & security management

- ***Key Performance Indicators*** (KPIs) are used to help organizations understand how well they are performing in relation to their strategic goals and objectives.
- KPIs provide the most important performance information that enables organizations and their stakeholders to understand whether the organization keeps track in realization of relevant activities and processes or not.
- The goal is to develop a set of KPIs for given organization to reduce the complex nature of organizational performance to a small number of key indicators in order to make the management problem more understandable and transparent for decision making.
- KPIs can be counted and compared; it provides evidence of the degree to which an objective is being attained over a specified time. The issue is whether to use ***qualitative or quantitative metrics***.
- Due to complexity of real technical systems the evaluations are often most powerful for decision making when the analysts use ***both qualitative and quantitative metrics***.

Category A of Controls / Barriers (C/B) for defining KPIs

A1. Leadership and integrated management - *based on systemic MTE approach,*
A2. Organisational culture - human resources and competencies, permits to work and change management, procedures and training,
A3. Design, modernisation and performance of installations - including infrastructure and protections, redundancy and separation of equipment,
A4. Operational Technology (OT) - operational control and interfaces, OT performance, safety and security,
A5. Information Technology (IT) - information storage, transfer and interfaces, IT *performance, safety and security,*
A6. IACS design and performance - requirements / criteria for functional safety (PL/SIL) and security (SL, SAL) solutions,
A7. Alarm system (AS) - design concept and performance, procedures and operator interface and training,
A8. Maintenance - including calibrations, functional tests and preventive maintenance based on statistics available and plant specific reliability data,
A9. Evaluation of near misses and abnormal states of minor consequence registered (MCR), injuries / fatalities,
A10. Fire monitoring and protection system - design concept, inspections, tests and preventive maintenance.

Category B of Controls / Barriers (C/B) for defining relevant KPIs

For hazardous plants (e.g. / SEVESO / COMAH type) additional C/B categories are proposed to be considered for defining relevant KPIs:

B1. Safety and security culture in organisation,

B2. Integrated management system *(IMS)* - oriented on evaluations of risks, based on processes / procedures and requirements / criteria, covering the quality, occupational health and safety, environmental, reliability, safety and security aspects; ISM audits and improvement plan,

B3. Leading and lagging indicators - for tiers: 1, 2, 3 and 4,

B4. Emergency and evacuation procedures and exercise plan.

Examples of KPIs for B3 subcategory

Fatality or injury to employee or contractor

Tier 1 KPI: Fatality and/or lost workday case - days away from work or *lost time injury* (LTI).

Tier 2 KPI: Recordable occupational injury (restricted work case or medical treatment case).

Fatality or injury to third party

Tier 1 KPI: Fatality, or injury/illness that results in a hospital admission.

Tier 2 KPI: Informing about PSE (*process safety event*) and restricted area of admission.

Tier 3 KPIs:

- Number of operational errors due to incorrect/unclear procedures,
- Number of operational shortcuts identified by near misses and incidents,
- Number of PHA recommendations related to inadequate operating procedures.

Tier 4 KPIs:

- Percentage of procedures to be reviewed and updated versus plan,
- Percentage of procedures to be reviewed and updated after changes or corrections within P&ID and/or AS in relation to IACS.

Examples of security related performance indicators to be assessed in an insurance audit of oil port infrastructure

Physical Security (PS)
- physical security policy,
- enforcing a clear desk policy at sites, etc.

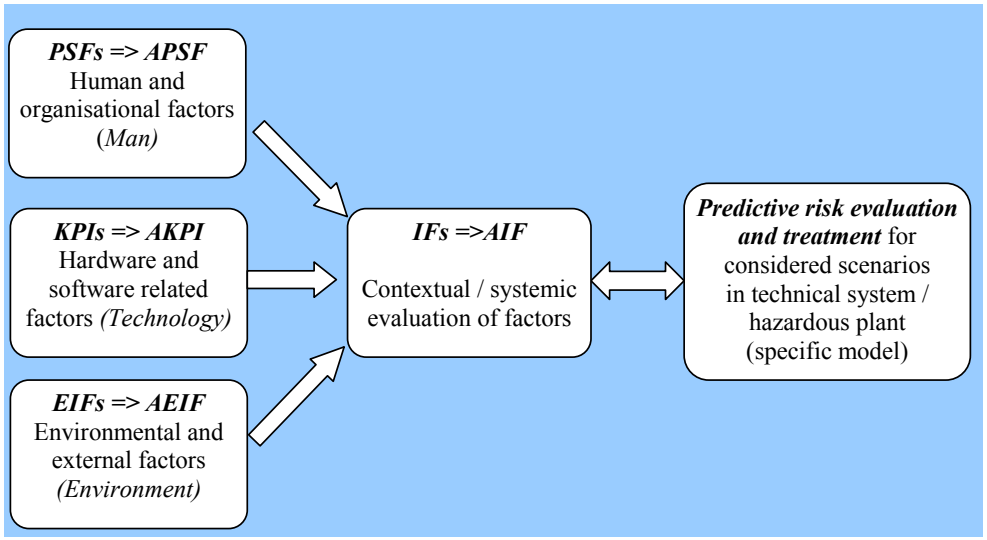
System Security (SS)
- firewalls in place at all external connection points,
- firewall rules, configurations and settings on at least a monthly basis,
- running anti-virus on system network including on all incoming traffic, etc.
- intrusion prevention, detection or data loss prevention software deployed on workstations and laptops,
- monitoring and reviewing intrusion logs (how often),
- expected response time for a critical alert,

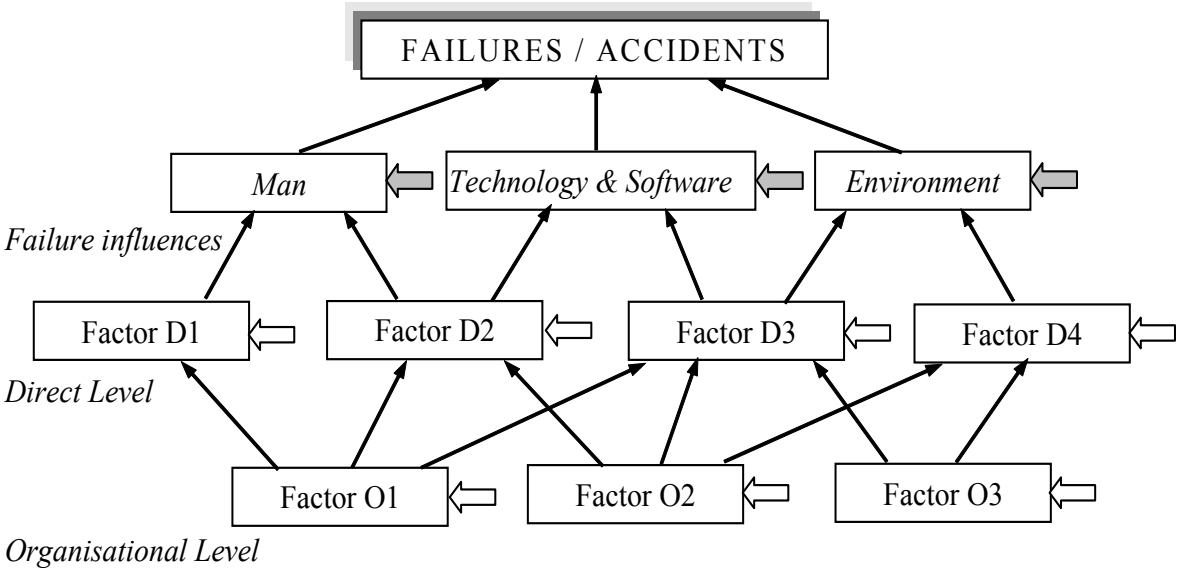
Network Assessment (NA)
- is the network externally assessed for penetration tests in last year?
- is the network internally assessed for penetration tests in last year?
- DMZ has been configured and tested in last year?

Remote Access (RA)
- remote access to your corporate network is allowed?
- if yes, do you limit to two–factor authentication only?
- all connecting devices are required to have anti-virus and firewall installed in accordance with the company policy for updates and patching?

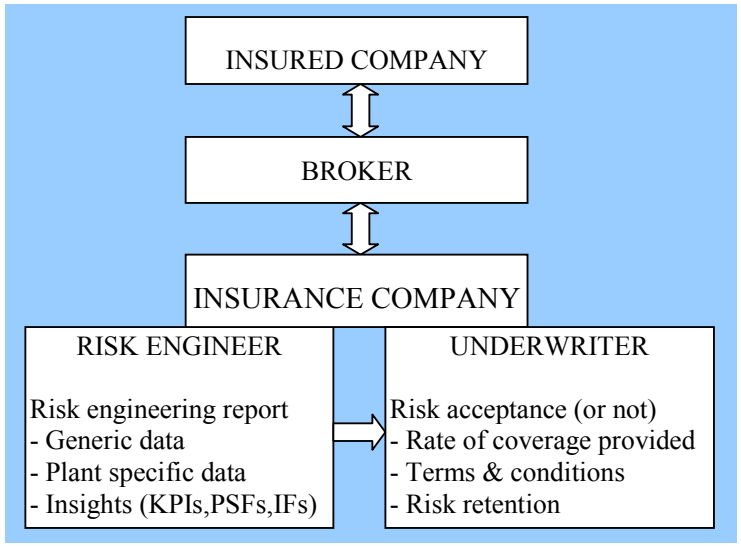
Risk Management (RM)
- procedures are available that govern RM?
- have you roles and responsibilities assigned that identify who is responsible for safety and security in your company?
- have you a dedicated technical team responsible for configuring IT security measures?
- do managers ensure that the requirements and criteria for acceptance of new systems are clearly defined, agreed, documented, and tested?
- is vulnerability management process regularly reviewed?

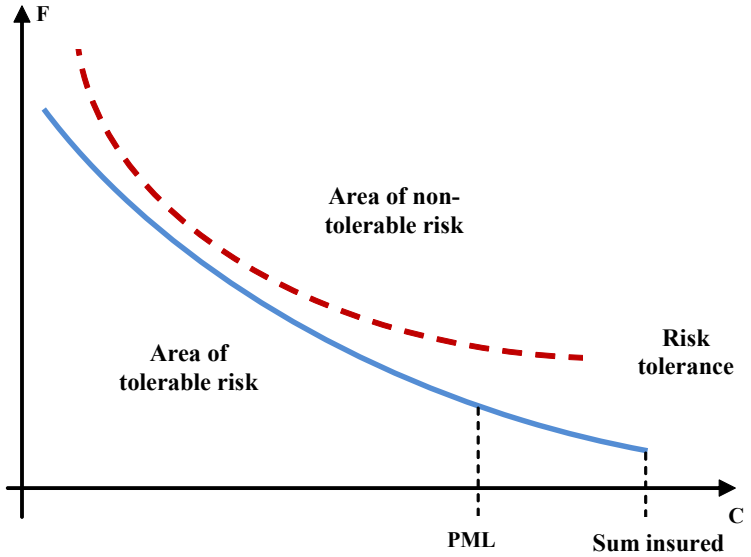
Towards systemic MTE approach in safety and security analysis and management in life cycle





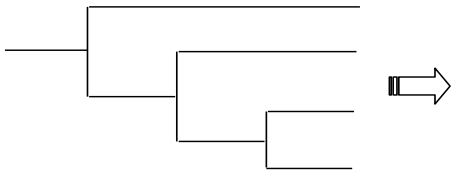
Evaluation of risks to be transferred to the insurance company (in context of insurance products available)

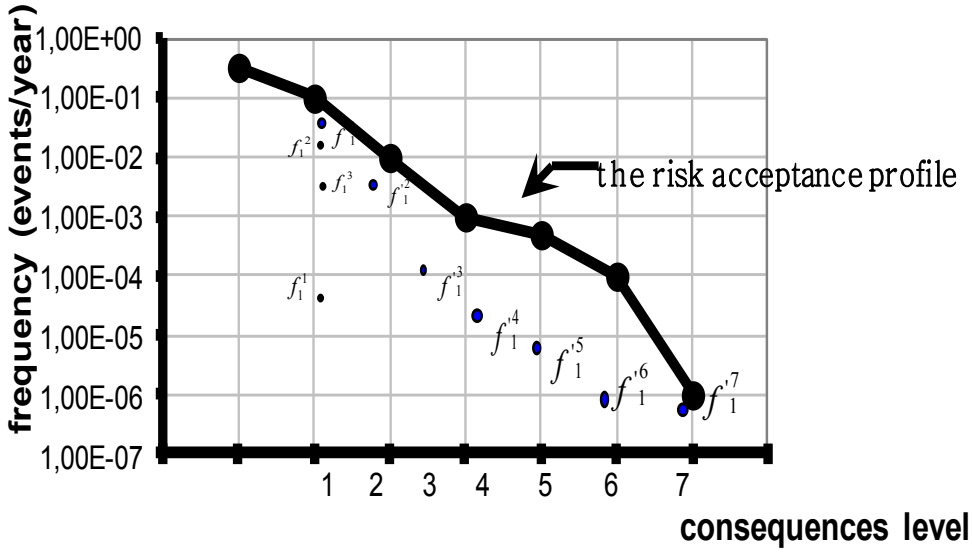




Probable Maximum Loss PML

Scenarios considered





Conlusions

The oil port reliable operation is crucial for the energy sector economy and state *critical infrastructure* (CI). There are numerous requirements, recommendations and guidelines how to design and operate hazardous plants and oil ports, with relevant installations and infrastructure, integrating in decision making the safety and security aspects .

Due to complexity of systems considered and many factors involved it is necessary to apply in practice a *process based management system* (PBMS) including *business continuity management* (BCM) and integrated *safety & security* (S&S) aspects.

The PBMS takes advantage of evaluating risks and KPIs with regard to quantitative and qualitative information (aggregation of expert opinions) to support effectively decisions concerning **reliability, safety and security** in an integrated way.

The methodology proposed is focused on the evaluation of IACS (*Industrial Automation and Control Systems*) and IT/OT convergence indicating how to integrate in evaluations the functional safety (EN 61508) and cyber security (IEC 62443) aspects. The approach is compatible with the Industry 4.0 concept being implemented nowadays in practice.

The insurance company point of view has been also considered, because nowadays the insurer, interested in decreasing risks, offers the expertise how to limit effectively some risks in life cycle from the design conceptual stage of hazardus plant, through its reliable and safe operation, until decommissioning.

Information

Details are given in Journal of Polish Safety and Reliability Association – JPSRA,

Special Issue on HAZARD Project,

Volume 10, No 1, April 2019

Slides below illustrate Laboratory LINTE^2
at Gdańsk University of Technology (GUT)
https://eia.pg.edu.pl/linte/main
designed and available at present for making experiments
in the domain of critical infrastructure - electric power systems
using advanced DCS/SCADA system
for verifying and validating control/protection algorithms
with regard security aspects to limit the network vulnerability

Basic information about the project

- Finanse source: POIG
- Budget: funding POIG 46,220 mln PLN, overall costs **50,953 mln PLN**
- Goal: construction of a new laboratory for R&D in area of electric power systems
- Completion of the investment: 31 December 2015
- Starting operation: 12 April 2016

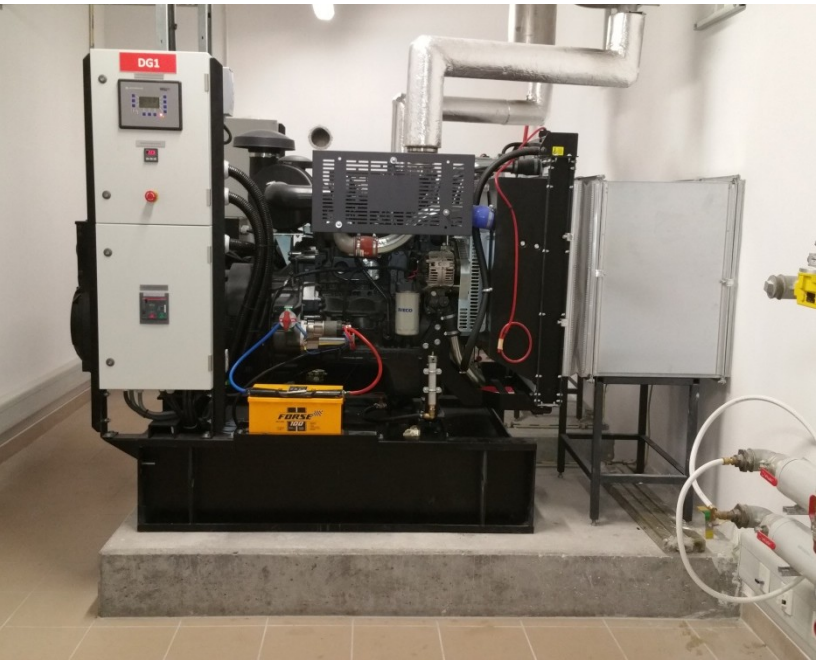
Control system and communication conduits

- 9 control rooms with operator workstations and SCADA software (remote supervising, development and initiating algorithms, on-line control, configurations, etc.)
- controllers of functional units (SJF) remoutly programmed from engineering stands (*Simulink Real Time*)
- 70 digital protection relays programmed from engineering stands

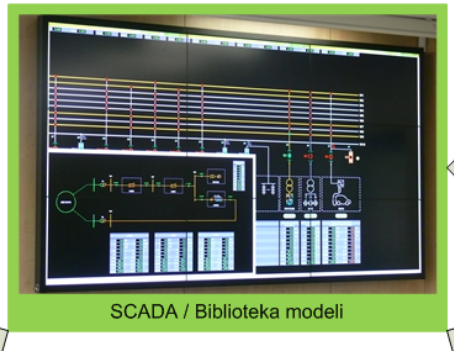
Main hall of the laboratory

Functional units

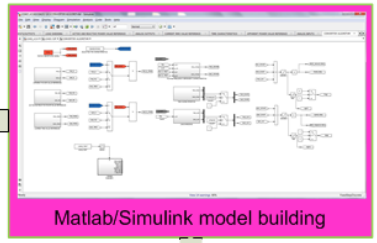
- Autonomus energy sources:
  - Solar power station 33 kW
  - 2 generating sets 80 kW with Diesel engines
  - gas microturbin 65 kW



Design of experiments



Simulink Real-Time model files (*.dlm)



Simulink Real-Time Explorer

Ethernet / IEC 61850

Ethernet / Simulink Real-Time API